Amendments to the Claims

Please amend Claims 1, 10, and 12. The Claim Listing below will replace all prior versions of the claims in the application:

Claim Listing

OK to ENTER /JM/

1. (Currently amended) An agent process for controlling access to digital assets in a network of data processing devices, the process comprising:

defining a ~~point-of-use~~ security perimeter that includes ~~the operating system kernels of~~ two or more data processing devices in the network, each of the data processing devices including an operating system kernel, and at least one of the data processing devices being a user client device having access to a digital asset;

defining one or more policy violation predicates ~~that serve to~~ implementing policy logic to control access to ~~and that are asserted at the point-of-use of a digital asset upon an occurrence of a possible risk of use, outside of the security perimeter, of~~ the digital asset by an end user of the user client device;

sensing atomic events within [[an]] the operating system kernel of [[a]] the user client device, the atomic events being low level kernel events and being sensed upon actions relating to authorized access to [[a]] the digital asset by the end user of the user client device;

aggregating multiple atomic level events sensed within the user client device to determine a combined event; and

asserting a policy violation predicate, at the user client device, upon an occurrence of a combined event that violates ~~a predefined digital asset usage~~ the policy logic, the policy logic violation corresponding to ~~that indicates~~ a risk of use of the digital asset outside of the security perimeter.

2. (Previously presented) A process as in Claim 1 wherein the step of asserting the policy violation predicate is implemented in the operating system kernel of the client user device.

3. (Original) A process as in Claim 1 additionally comprising:

preventing a user from accessing the digital asset if the policy predicate indicates a violated policy.

4. (Original) A process as in Claim 3 wherein the preventing step includes an IRP intercept.

5. (Original) A process as in Claim 1 wherein the combined event is a time sequence of multiple atomic level events.

6. (Original) A process as in Claim 1 additionally comprising:

prompting a user to document a reason for a policy violation, prior to granting access to the digital asset.

7. (Previously presented) A process as in Claim 1 additionally comprising:

asserting multiple policy violation predicates prior to indicating a risk of use of the digital asset outside of the security perimeter.

8. (Original) A process as in Claim 2 that operates independently of application software.

9. (Original) A process as in Claim 1 additionally comprising:

notifying a user of a policy violation, and then permitting access to the digital asset.

10. (Currently amended) A process as in Claim 2 wherein the sens[[s]]ing, aggregat[[ors]]ing, and asserting steps operate in real time.

11. (Original) A process as in Claim 1 additionally comprising:

determining the identity of a particular file in the asset access event.

12. (Currently amended) A system for controlling access to digital assets in a network of data processing devices, the system comprising:

a digital asset usage policy server storing one or more digital asset usage policies programmed to be applied to a ~~point-of-use~~ security perimeter, the security perimeter comprising ~~the operating system kernels of~~ two or more data processing devices, each of the data processing devices including an operating system kernel, at least one of the data processing devices being a user client device having access to a digital asset, and the one or more digital asset usage policies implementing policy logic to control access to the digital asset by an end user of the user client device;

an atomic event sensor, the sensor located within [[an]] the operating system kernel within ~~an end~~ the user client device and programmed to sense atomic events within the operating system kernel, the atomic events being low level kernel events and being sensed by the sensor upon actions relating to authorized access to ~~one or more~~ the digital asset[[s]] by [[an]] the end user of the [[end]] user client device;

an atomic level event aggregator programmed to determine the occurrence of an aggregate event that comprises more than one atomic level asset access event sensed within the user client device; and

a policy violation detector programmed to determine whether an aggregate event has occurred that violates ~~a predefined digital asset usage~~ the policy logic, the policy logic violation corresponding to ~~that indicates~~ a risk of use of [[a]] the digital asset outside the security perimeter.

13. (Previously presented) A system as in Claim 12 wherein the policy violation detector is located in the operating system kernel of the user client device.

14. (Previously presented) A system as in Claim 12 wherein the policy violation detector is programmed to determine a violated policy type.

15. (Previously presented) A system as in Claim 14 wherein the policy violation detector includes an IRP intercept.

16. (Previously presented) A system as in Claim 12 wherein the combined event is a time sequence of multiple atomic level events.

17. (Previously presented) A system as in Claim 12 further including a user interface within the client device programmed to require the end user to document a reason for a policy violation prior to granting access to the digital asset.

18. (Previously presented) A system as in Claim 12 wherein the policy violation detector is additionally programmed to assert multiple policy violation predicates prior to indicating a risk of use of the digital asset outside of the security perimeter.

19. (Previously presented) A system as in Claim 13 that is programmed to operate independently of application software.

20. (Previously presented) A system as in Claim 12 wherein the user client device includes a user interface programmed to notify the end user of a policy violation and to permit access to the digital asset once a reason for the violation is provided by the end user.

21. (Previously presented) A system as in Claim 12 wherein the sensor, aggregator and detector are programmed to operate in real time.

22. (Previously presented) A system as in Claim 12 wherein the detector is additionally programmed to determine the identity of a particular file in the atomic level asset event.